

NAVAL WAR COLLEGE
Newport, R.I.


WEAPONS OF MASS DESTRUCTION
A NETWORK-CENTERED THREAT

by

D. G. Diggs
Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.



18 May, 1998

Captain W. M. Piersig, USNR
Commander G. P. Davis, USN

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): Weapons of Mass Destruction a Network-Centered Threat (U)			
9. Personal Authors: CDR D.G. Diggs, USN			
10. Type of Report: FINAL		11. Date of Report: 18 May 1998	
12. Page Count: 22			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: Battlespace Dominance; Weapons of Mass Destruction; Network Centered Threat; Information Warfare; Initiatives; policy; doctrine			
15. Abstract: Battlespace dominance is more than the physical control of air, land and sea. Under the network-centric concept of operations, U.S. forces must be ready to control the infosphere in order to assure military objectives can be achieved. Perhaps the most effective information warfare (IW) weapon is a Weapon of Mass Destruction (WMD), specifically a biological or nuclear weapon. Important questions should be answered about the ability to protect American information networks from the significant information disruption characteristics of WMD.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Abstract of

WEAPONS OF MASS DESTRUCTION
A NETWORK-CENTERED THREAT

Battlespace dominance is more than the physical control of air, land, and sea. Under the network-centric concept of operations, U.S. forces must be ready to control the infosphere in order to assure military objectives can be achieved. Perhaps the most effective information warfare (IW) weapon is a Weapon of Mass Destruction (WMD), specifically a biological or nuclear weapon. Important questions should be answered about the ability to protect American information networks from the significant information disruption characteristics of WMD.

The increasing number of WMD capable nations is casting a growing shadow across regions of importance to the United States and presenting a significant physical threat to performance of critical operational functions like logistics sustainment and force protection. More significantly, WMD threatens the movement of information through the sensor, information, and target grids (collectively known as C4ISR for Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance) of American forces. Only through complete battlespace dominance, including control of the infosphere, through any climate or environmental condition, can the United States hope to deter an adversary from employing WMD.

Initiatives discussed in this paper represent elements in an investment strategy in support of the current focus of Joint Vision 2010. The key to protecting information networks centers on sound deterrence strategy, infrastructure and force protection policies, and doctrine supporting conventional warfare operations in a WMD environment.

WEAPONS OF MASS DESTRUCTION

A NETWORK-CENTERED THREAT

Introduction

"Now an army may be likened to water, for just as flowing water avoids the heights and hastens to the lowlands, so an army avoids strength and strikes weakness." Sun Tzu

This paper focuses on the impact of Weapons of Mass Destruction (WMD), not against physical targets, but against the information networks upon which American military forces are increasingly reliant. Joint Vision 2010's conceptual framework for the future conduct of military operations leverages technology and joint operations to achieve battlespace dominance. The basis for this framework, improved command, control, and intelligence is assured through information superiority.¹ Perhaps the most effective information warfare (IW) weapon is WMD, specifically biological and nuclear weapons, which applied against key strategic targets could paralyze information flow. This 'movement of information' constitutes a critical vulnerability for American fighting forces. WMD warfare, conducted against American information systems, may pose, perhaps, the only true current threat to U.S. freedom of action in the world.

America's conventional superiority is forcing potential national and transnational adversaries to consider alternate approaches to countering American strength. It is unlikely that the United States will face another adversary like Saddam Hussein who attempted to stand firm against America's conventional forces. Rather, adversaries will avoid American strength and attempt to exploit weakness. It is likely that adversaries in the future will attempt to equalize the battlefield by orchestrating campaigns using WMD for information disruption. Increasingly, a growing number of WMD capable nations will cast their shadow across regions of importance to the United States. This WMD shadow will present significant physical threats to the

performance of critical operational functions like logistics sustainment and force protection. More significantly, however, WMD will threaten the movement of information through the sensor, information, and target grids (collectively known as C4ISR for Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance) of American forces. Serious thought must be given on how to counter this threat. Adversaries must be dissuaded from pulling the WMD trigger while conventional forces must be prepared to operate in regions under a WMD shadow.

National Military Strategy tasks the Armed Forces with deterrence of armed conflict and should deterrence fail, to fight and win. The retention of American nuclear weapons represents a key component of the nation's WMD deterrence policy.² However, a credible deterrence strategy and supporting operational doctrine for America's employment of nuclear weapons have not been developed. Additionally, conventional military doctrine, increasingly reliant on information flow and "network-centric" concepts may not be sufficient to either deter, or fight and win, in a theater in which WMD has been introduced by an adversary. It is critical that the United States develop effective deterrence and warfighting strategies and doctrine to counter this threat. Specifically, conventional forces should be prepared to dominate the infosphere—the realm through which all information flows—even in a WMD environment. To assure a credible deterrence, or failing deterrence, to provide American fighting forces the ability to conduct operational functions in any environment, the battlespace picture must remain clear and the decision making process intact.

Network-Centric Revolution

"We are in the midst of a revolution in military affairs (RMA) unlike any seen since the Napoleonic Age, when France transformed warfare with the concept of levee en masse . . . a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare." Vice Admiral Cebrowski

Sustained by success in the Persian Gulf War and guided by Joint Vision 2010 as a conceptual template, United States military forces have revolutionized warfighting. Leveraging technology to gain exponential improvements, they are doing more with less and are simply better and faster at accomplishing critical operational functions than potential adversaries. Never before has a military force been as capable of engaging and dominating an adversary and sustaining operations over long distances for extended durations. Increasingly, this new style of warfare is referred to as "network-centric."³ Linked together by networks of shared sensor, information, and targeting grids, American fighting forces are achieving total battlespace dominance, striking precisely at enemy vulnerabilities in synchronized and joint operations. Networked together, strike operations have been transformed from the massing of forces to the target to the massing of effects from dispersed forces upon a target. The whole becomes greater than the sum of its parts—the battlefield picture is understood by every element.

History teaches, however, that an advantage in technology and weapons systems do not assure victory. The strategy used by an enemy may not be consistent with one's preconceived conceptions of the future battlefield. In Napoleonic times, despite relative parity in weapons between European nations, the French *levee en masse* altered force employment concepts and transformed the conception of France as a militarily weak and ineffective opponent. In World War II, Nazi Germany's *blitzkrieg* caught France unprepared and unable to cope with the rapidly-changing battlefield. Relying on World War I as a model, the French heavily committed to the concept of defensive war. Again, despite relative military parity in weapons technology,

France fell years behind German operational strategy and suffered quick defeat.

J.F.C. Fuller's contention that every weapon develops a counter-weapon suggests a cyclical balance in war between offense and defense.⁴ The United States today is focused on new offensive capabilities enabled by information technologies and precision guided munitions (PGMs). America may be neglecting, however, the "defensive" lessons gleaned from the Persian Gulf War by potential adversaries. Preconceived American concepts of battlespace dominance, reliant on information flow, may not be sufficient. Future adversary's may attempt to equalize the battlefield by orchestrating campaigns coupling WMD use with information disruption. Current national military strategy places great emphasis on the maintenance of a capability to project power on significant scale. Under Joint Vision 2010, network-centric warfare provides the organizing principle for the operational concepts which are enabled by information superiority.⁵ The strategy—massing weapon effects without massing forces (thus minimizing vulnerability)—is increasingly viewed under system or network-centric paradigms. Information flow, however, may well become a critical vulnerability to America's ability to wage war.⁶

Network-Centered Threats

"[An information warfare] campaign will become increasingly likely. Probable scenarios could couple an attack using chemical or biological weapons with information disruption of the warning and response processes." 1997 Defense Science Board - DoD Responses to Transnational Threats

Third World nations and transnational actors require very little in the way of technology or money to develop and employ many forms of WMD. Further, they can upgrade their Command, Control, Communication and Intelligence (C3I) architectures by applying the rapidly developing global information infrastructure, increased freedom of the press, Global Positioning Satellites (GPS), and commercial imagery⁷. Together, these capabilities give nations and transnational

actors weapons and information access that surpass all threats from the former Soviet Union with the exception of global nuclear war. Given the rapid proliferation of weapons and technology, the chances of Americans facing biological or nuclear weapons is probably greater today than anytime in history. The United States must prepare to face adversaries who, unable to match the United States in technological power or resources, might be willing to use WMD to achieve their objectives. We must prepare for the enemy's weapon of choice.

Andrew Krepinevich concluded a study on "military revolutions" in part by stating that it is by no means certain that competitors will follow the same path as the United States when undergoing a revolution in military affairs (RMA).⁸ Different security requirements, cultures, economic situations and objectives may lead to different ways of exploiting and integrating technology into military affairs. Consider the impact the following hypothetical attack on American information capabilities by an enemy using WMD:

Days before the expected commencement of Gulf Thunder (bombing campaign), a small crop-duster aircraft flies over Washington, D.C. releasing botulinum—one of the most poisonous substances known and fatal within three days to up to 80% of those exposed. With little history of integrated federal, state and local law enforcement planning or strategy, officials are immediately at a loss for procedures.⁹ Local medical facilities with no experience in treating large numbers of biologically affected people are overwhelmed and unable to coordinate a response. The population panics. Washington, D.C. virtually shuts down with officials unable to respond to the crisis. Two anonymous militia groups claim responsibility and promise further attacks creating panic in other large cities. While there is suspicion of Gulf nation involvement, it cannot be immediately confirmed.¹⁰

Five days later, two nuclear weapons are launched from the Gulf nation and detonated at a high altitude (approximately 100 kilometers) over the Gulf nation airspace. The detonations generate a powerful electromagnetic pulse (EMP) that instantaneously shorts out unprotected electronics networks in the theater of operations. The Gulf nation declares the weapon detonations as "tests" conducted over their own territory to validate defensive capabilities in light of the overwhelming U.S. military build-up in the region.¹¹ While producing no direct lethal damage to troops or local populations, significant damage is done to American sensors and information and communication architectures. Information gained from satellites, airborne platforms, and ground stations is disrupted leaving the U.S. blind in the region and with communications to and from Central Command (CENTCOM) Headquarters significantly

disrupted. Electronic components in advanced weapons systems and transportation vehicles are also damaged. It is believed that EMP has not degraded, to the same degree, the less sophisticated Gulf nation equipment.

WMD employed as in this increasingly credible scenario, and specifically targeted against American information dominance, effectively would disrupt key informational network grids including connectivity, sensors, C2 nodes, information systems, transmitters and receivers. Colonel John Warden, in discussing the strengths of the strategic application of air power, advocates viewing the enemy as a "system composed of numerous subsystems."¹² Further, he stresses that once this "system" concept is understood, identification of key strategic targets (those which can paralyze the system) should be hit simultaneously, depriving the enemy of the opportunity to respond effectively. Near simultaneous attacks on American strategic and operational level vulnerabilities, such as in this hypothetical scenario, might allow an adversary to paralyze American command and control. If the enemy can interrupt or degrade America's national command nodes and theater information grids, he can effectively blur the battlespace picture and disrupt the decision making process.

The Strategic Context — Deterring WMD

"The primary task of the Armed Forces will remain to deter conflict . . ." Joint Vision 2010.

Because United States Armed Forces will increasingly be called upon to conduct operations against WMD equipped nations, it is critical that regional and national deterrence strategies are developed. Many believe that overwhelming American nuclear superiority will deter an adversary from using WMD against American interests. However, successful

deterrence requires that the threat to retaliate be effectively communicated to an adversary and that he is convinced the promised action will cost him more than WMD employment would gain. The threat must be credible and the force for retaliation must be capable of achieving its aim. It is arguable whether United States deterrence strategies fulfill these objectives.

The threat of Iraq's use of WMD in the Persian Gulf War was taken seriously.

CENTCOM's February situation report stated "We expect Iraq to initiate chemical operations within 24 hours."¹³ Despite this, a study of the resulting actions of national decision makers exposes their inability to agree on a deterrence strategy. While the United States vaguely communicated a threat of retaliation to Iraq, it was unlikely that threat was credible. Disruption of carefully crafted coalitions coupled with a United States pledge never to use nuclear weapons on a non-nuclear nation reduced U.S. retaliation options. Additionally, deterrence must be credible not only to an enemy, but also represent credible U.S. policy. In his memoirs, former Secretary of State James Baker labeled U.S. nuclear policy in the Persian Gulf as "calculated ambiguity"—ambiguous because it gave the impression that the use of chemical or biological agents by Iraq would result in U.S. nuclear retaliation. American ambiguity, however, created a paradox; despite hinting at the possibility of using nuclear weapons, there was never any plan to resort to nuclear weapons.¹⁴ Discussions were conducted on possible EMP strikes by U.S. forces and the use of nuclear weapons on biological targets (to generate high heat levels to destroy stored biological agents), however, there was no formal planning guidance issued to the Pentagon.¹⁵ In short, while the possible use of nuclear weapons as a deterrence might today exist in the mind of an adversary, ambiguity exists within military planning circles.

The demise of the Cold War bipolar system resulted in disintegration U.S. policy concerning employment of nuclear weapons for deterrence—deterrence is no longer firmly rooted the use of nuclear weapons. Despite policy statements supporting retention of nuclear weapons as a key component of the nation's WMD deterrence policy, employment plans and operational doctrine have yet to be coordinated. Specifically, C3I doctrine required to support tactical nuclear deterrence policy does not exist and employment plans to govern the use of strategic nuclear weapons in a region in which American or coalition forces are conducting operations have not been developed. Additionally, the capability of the United States to conduct nuclear retaliation strikes has become more difficult. Military draw-downs and the post-Cold War de-emphasis on nuclear weapons have resulted in a gradual loss of theater-level capability and expertise. Integrated and sequential plans for the limited employment of nuclear weapons in pursuit of an agreed upon strategic objective do not exist, nor are they under discussion.

In his classic work on nuclear strategy, Henry Kissinger stated: "Perhaps the basic problem of strategy in the nuclear age is how to establish a relationship between a policy of deterrence and a strategy for fighting a war in case deterrence fails." Dr. Kissinger struggled with the problem of ultimate weapons in limited wars and concluded that "a deterrent which one is afraid to implement when it is challenged ceases to be a deterrent."¹⁶ Today there is no well-vetted, overarching national deterrence strategy for deterring an adversary's use of WMD, conventional or nuclear. Essentially, U.S. policy has come full circle from the earliest days of nuclear strategy when presidents would introduce vague nuclear threats for the political imperative of blocking an adversary's objective without considering, if the threat failed, the implications of lost deterrent credibility (if nuclear weapons were not used) or the consequences of nuclear weapon

use.¹⁷

Finally, deterrence requires an ability to exert influence over an adversary. Deterrence assumes rationality—an adversary must be capable of being deterred. Many nations, however, have vastly different frames of reference and different concepts of rationality than that which the United States encountered from the Soviet Union. Irrational enemy leaders, different value hierarchies, or the perception that any exchange of WMD could discredit American diplomacy could all lead to employment of WMD by an adversary. Also, deterrence may prove ineffective against terrorists and rogue nations who do not always present clear objectives for U.S. “punishment” strikes.

Potential regional adversaries of the United States are acquiring WMD arsenals and associated long range delivery systems in an attempt to counter the strategic and military operational advantage of U.S. power projection. Serious thought must be given how to dissuade a nation from pulling the WMD trigger. Additionally, it is critical that, when actual employment of WMD by an adversary is encountered, the United States is prepared to “fight and win.” In addition to the inability of national decision makers during the Persian Gulf War to agree on deterrence strategy, they were unable to concur on a specific response to a possible Iraqi employment of WMD. One must question if the current lack of a sound nuclear deterrent and the lack of a credible response may make the use of WMD by an adversary more likely. What is clear is that the United States does not want to set a precedent allowing use of WMD against American interests without a swift and violent response, even if that response is conventional. Conventional deterrence against WMD, if used in place of nuclear deterrence, must convince a potential WMD adversary that the United States is capable and willing to punish.

Operations Under the Shadow . . .

" . . . but should deterrence fail, to fight and win our nation's wars. " Joint Vision 2010

Inability to conduct key operational functions during any phase of military operations could quickly neutralize American force advantages and equalize the battlefield. WMD, both nuclear and biological, serve as an effective conventional IW weapon by strategically and tactically disrupting command and control. Nuclear weapons can destroy personnel and facilities and disrupt telecommunications equipment and computers. Networks are especially vulnerable to nuclear electromagnetic pulse (EMP) attack. High voltage bursts of energy, similar to a lightning strike, occur in conjunction with a nuclear blast, and can effectively cripple communication networks, power grids, and transportation vehicles. Especially susceptible may be firmware-based storage systems (ROM, EPROM, etc.) which are critical to many computer-based systems operated by military forces today. Additionally, EMP could effectively disable low-Earth orbit sensor satellites which are not radiation hardened. An EMP strike over a battlefield could effectively bring an end U.S. battlespace dominance without harming a single person.¹⁸

The impact of biological weapons on a theater of operations has yet to be fully assessed, however, they would likely be extremely effective at eliminating key nodes within information networks. Simple biological agents might be used to close airfields from which key sensor and C3I aircraft like AWACS or JSTARs operate, eliminate headquarters facilities either in a theater or deep in the rear (including Washington, D.C. itself), or cripple transmission and receiver sites

required to move information from sensor to commander or commander to shooter.

Today's capability to project conventional forces in nuclear and biological WMD environments lacks key protection features. Virtually no operational doctrine for employing forces in a region under a WMD shadow exists. Especially vulnerable are C4I capabilities. While military strategic nuclear C3 systems in the past were radiation hardened, the new reliance on commercial off-the-shelf (COTS) and commercial communications systems leaves the military extremely vulnerable. To assure American conventional forces can achieve Joint Vision 2010 operational concepts, network-centric infrastructure protection must be provided for information flow. Battlespace dominance is more than the physical control of air, land, and sea. Under the network-centric concept of operations, U.S. forces must be ready to control the infosphere. Only through complete battlespace dominance, including control of the infosphere, through any climate or environmental condition, can the United States hope to deter an adversary from employing WMD.

Counter-WMD Strategy — Concepts for Force Employment

"The immediate and prolonged effects of WMD . . . pose unprecedented physical and psychological problems for combat forces and non-combatant populations alike. Not only must U.S. forces be prepared to survive and perhaps operate in a WMD environment for long periods of time, they must also have effective, sustained C4I to accomplish their missions." Joint Pub 3-12

Few things would be more likely to invite a WMD attack by an adversary than the prospect of paralyzing an American response. To ensure retaliation, it is important that the United States develop capabilities which will allow power projection into a WMD environment and preserve enough strength to inflict a swift and violent counterattack on an adversary. There are three

key requirements for integrating survivable and reliable operations into today's force structure: development of a reconstitution capability following a WMD attack for both C2 and fighting forces, integration of a thin-line architecture of current C4I systems, and development of WMD warfare operational doctrine.

Reconstitution of personnel and facilities following a WMD attack should be conducive to allowing an operational commander to plan, conduct, and sustain the full spectrum of military operations. Specifically, reconstitution should protect America's capability to continue the fight, gain positional advantage over an enemy, and concentrate surviving forces on decisive points. Further, reconstitution should assure the capability to conduct additional key operational functions like force protection, logistics support, and intelligence collection.

Theaters in which troops are introduced should have, in addition to the established information infrastructures, survivable C4I systems which provide a thin-line capability throughout a WMD attack. Any such infrastructure must be sufficient to absorb a WMD first-strike and assure a residual capability sufficient to ensure a retaliation with enough strength to inflict unacceptable damage on an adversary.

Finally, critical to WMD-shadowed warfare is the development of preplanned operations which ensure a ready conventional force capable of executing C2, maneuver, strike, and logistics sustainment in any WMD environment. Procedures must be incorporated into doctrine and identify threats, capabilities, postures, and budget issues.

Applying the Resources

"We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Joint Vision 2010

Many of the old distinctions between "strategic nuclear" warfare and "theater" warfare have disappeared. However, the Cold War divisions between conventional and strategic nuclear forces remains in place today stifling creative thinking by OSD and Joint Staff planners. The problems encountered by the introduction of conventional forces into regions under a WMD shadow are well understood by the nuclear hardening community, specifically the concept of survivable C4I capability. Forces established to fight strategic nuclear war today operate systems capable of moving information despite EMP disruption and have for years focused on providing robust and redundant C3 under the most difficult of environments— nuclear warfare. Conventional warfighters, however, have yet to design, or even articulate, what it would take to protect a core of critical modern conventional technology systems against varied WMD threats. Like their strategic warfare counterparts, conventional planners should identify the minimum amount of equipment most critical to carrying out anticipated plans. This equipment should be hardened against WMD effects (most notably EMP).

In their book "Strategic Information Warfare; A New Face of War" the authors, while addressing vulnerabilities in national information infrastructures, endorse the concept of a minimum essential information infrastructure (MEII) similar to survivable networks established for strategic nuclear connectivity.¹⁹ Instead of development of a federally owned MEII, which would be cost prohibitive, they recommended that the government fund a thin-line radiation-hardened program (radiation hardening would not be feasible for entire system). One way to construct an MEII, for example, would be to identify important areas of overlap between

traditional strategic infrastructures and requirements for operating conventional military forces in WMD-shadowed theaters. Additionally, degradation of information networks to the effects of WMD could be minimized during the development stage of new systems. Because it is far less expensive to design equipment initially to operate in an EMP environment than to retrofit such a capability, government incentives or funding might help minimize the impact of the integration of hardening into COTS systems. Finally, constructing a mixture of procedures, regulations, and tax incentives to support civilian efforts to protect their infrastructures might encourage owners and operators of the various national infrastructures to take measures to reduce their vulnerability and/or to ensure rapid network reconstitution if attacked.²⁰

General Colin Powell commented that at the height of the Persian Gulf War, “the automated message information network passed nearly two million packets of information per day [and] proved to be a vital margin that saved lives and helped achieve victory.”²¹ Technology has provided solutions to many of this nation’s conventional warfighting problems by providing American fighting forces information dominance over a battlefield. In order to protect this advantage, the United States should minimize the effectiveness of WMD as an IW weapon. If an enemy is able to disrupt either the connectivity between nodes or the ability to fuse the information, America’s advantage may be lost. Efforts should be made to develop a capability to operate effectively under WMD conditions before America begins total reliance on unprotected network-centric concepts.

Conclusion

"... one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed. Clausewitz

It will become increasingly difficult for the United States to delay or stop adversaries from developing WMD programs. The unprecedented proliferation of weapons-grade uranium and plutonium and the diffusion of chemical and biological capabilities to the Third World have significantly increased the possibility of a WMD incident.²² The magnitude of Iraq's NBC program astounded the United Nations Special Commission (UNSCOM) when, following the Persian Gulf War, documents and materials were discovered that indicated advanced nuclear and biological programs.²³ India's recent nuclear tests serve as further evidence of the United States' limited influence in stopping the proliferation of nuclear weapons.

Throughout the Cold War, America demonstrated credible determination to retaliate in kind against any use of nuclear weapons against U.S. interests. A nuclear deterrence policy was clearly spelled out for allies and enemies alike and exercised at the tactical levels. Today, the credibility that the United States will respond to WMD employment by an adversary with nuclear weapons has eroded. A coherent and well-vetted national nuclear deterrence policy against a WMD capable adversary should be reestablished by development of policy that includes limited tactical nuclear strikes or strategic nuclear weapon strikes in support of WMD deterrence.

Further, America's capability to respond conventionally, even under a WMD shadow should be protected. The Secretary of Defense has taken the initial steps to address force protection adding one billion dollars to chemical and biological defense programs as recommended by QDR.²⁴ Plans should also be developed to reconstitute a thin-line system of

“network-centric” capability and include CINC deployable C3 packages with a mixture of air, ground, and sea based elements that are resilient in a nuclear disturbed environment and that can remain clear of potential biological strikes (airborne or sea assets). These systems could also be available for CONUS emergencies and the reestablishment of civil C3 in the event of nuclear or biological weapons attacks directly on the North American continent.

Finally, doctrine supporting conventional warfare operations in a WMD environment should emphasize a reconstitution capability of theater and national level command and the ability to carry out command functions during and after a WMD strike. Ultimately, it will be the capability to support and sustain command and control capabilities, even in a WMD environment, that will assure continued U.S. freedom of action in the world. WMD warfare, conducted against American information systems, will still pose a threat to conventional and strategic forces, but will not be able to eliminate information superiority and the advantages gained through implementation of the Joint Vision 2010 concepts.

Before the U.S. military rushes forward to totally embrace network-centric technology, important questions should be answered about the ability to protect these networks from the significant information disruption characteristics of WMD. Networks, should they become the “hub of all power,” may come to represent America’s critical vulnerability. Initiatives discussed in this paper represent elements in an investment strategy in support of the current focus of Joint Vision 2010. The key to protecting information networks centers on sound deterrence strategy, infrastructure and force protection policies, and doctrine supporting conventional warfare operations in a WMD environment.

NOTES

1. Joint Chiefs of Staff. Joint Vision 2010, 19.
2. The White House. A National Security Strategy For A New Century. (Washington, D.C.: May 1997), pg. 9. Joint Chiefs of Staff. Doctrine for Joint Nuclear Operations (Joint Pub 3-12)(Washington, D.C.: 18 December, 1995), pg. v.
3. The term network-centric is attributed to Admiral Jay Johnson by Vice Admiral Arthur Cebrowski. For a more complete discussion of the integration of technology into military informational processes and the shift away from platform-centric processes see Vice Admiral Cebrowski, "Network-Centric Warfare-Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 28-35.
4. Reid, Brian Holden Reid, "J.F.C. Fuller's Theory of Mechanized Warfare," The Journal of Strategic Studies, December 1978. Vol. 1, No. 3, pg. 296.
5. "Observations on the Emergence of Network-Centric Warfare." Information Paper. <<http://www.dtic.mil/jcs/j6/education/warfare.html>> (27 Apr 98), pg 1.
6. Defense Science Board 1997 Summer Study Task Force, DoD Responses to Transnational Threats (Washington, D.C.: October 1997, pg. xiii.
7. Defense Science Board 1997 Summer Study Task Force, DoD Responses to Transnational Threats (Washington, D.C.: October 1997, pg. vii.
8. Andrew Krepinevich, "Calvary to Computer: The Pattern of Military Revolutions" in Strategy and Force Planning, 444-445.
9. Defense Science Board 1997 Summer Study Task Force, DoD Responses to Transnational Threats (Washington, D.C.: October 1997, pg. 3.
10. This biological scenario is similar to a drill run by the government to assess readiness to deal with a terrorist biological attack. Results of a simulated attack with smallpox hybrid virus dropped along the Mexican-American border resulted inability of authorities to coordinate relief efforts or to coordinate medical support to the area. For more information on the government exercise see Frank Gaffney Jr, "Biological Warfare Warning," Washington Times, April 28, 1998, pg 21 Report: U.S. Germ Attack Simulation a Disaster, New York Times, April 26, 1998. American intelligence warned in October 1990 that Iraq's botulinum capability was sophisticated enough to begin causing allied casualties within four hours. See Rick Atkinson, Crusade, The Untold Story of the Persian Gulf War, (New York: Houghton Mifflin Company, 1993), 88.

11. Although the specific effects on sensor, information, power and target grids is unknown, experts agree that an EMP attack, such as the one postulated in this scenario, would be devastating. For more discussion on EMP to unprotected electronic networks see Joseph C. Anselmo, "U.S. Seen More Vulnerable to Electromagnetic Attack," Aviation Week & Space Technology, July 28, 1997, pg 67.
12. Colonel John A. Warden III, USAF, "The Enemy as A System," Airpower Journal, Spring 1995, pg 42.
13. William M. Arkin, "Calculated Ambiguity," Washington Quarterly, Autumn 1996, pg 7.
14. *ibid.* pg 13.
15. Robert, S. Norris, "To Nuke or Not to Nuke," The Bulletin of the Atomic Scientists, January/February 1994, pg. 64.
16. Henry A. Kissinger, Nuclear Weapons and Foreign Policy (New York: Harper & Brothers 1957), 134.
17. Richard K. Betts, Nuclear Blackmail and Nuclear Balance (Washington, D.C.: The Brookings Institution 1987), 213.
18. Joseph C. Anselmo, "U.S. Seen More Vulnerable to Electromagnetic Attack," Aviation Week & Space Technology, July 28, 1997, pg 67.
19. Roger C. Molander and others, Strategic Information Warfare (Santa Monica, CA: RAND, 1996), 31.
20. *ibid.* pg 37
21. Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (Joint Pub 6-0)(Washington, D.C.: 30 May 1995), pg. II-1.
22. Henry Bartlett et al. "The Spectrum of Conflict: What Can It Do for Force Planners?" in Strategy and Force Planning, 411.
23. Ambassador Rolf Ekeus, "Beware Iraq's Biowar Legacy," Jane's IDR Extra, Vol. 2, No. 2, February 1997, Viewpoint.
24. Defense Science Board 1997 Summer Study Task Force, DoD Responses to Transnational Threats (Washington, D.C.: October 1997, pg. xiii.

Bibliography

- Anselmo, Joseph C., "U.S. Seen More Vulnerable to Electromagnetic Attack," Aviation Week & Space Technology, July 28, 1997, pg 67.
- Arkin, William M., "Calculated Ambiguity," Washington Quarterly, Autumn 1996, pp. 3-18.
- Atkinson, Rick, Crusade, The Untold Story of the Persian Gulf War. New York: Houghton Mifflin Company, 1993.
- Bartlett, Henry, Holman, G., Somes, Timothy. "The Spectrum of Conflict: What Can It Do for Force Planners" in Strategy and Force Planning, Edited by Strategy and Force Planning Faculty. Newport War College Press, Newport RI, 1997.
- Betts, Richard K. Nuclear Blackmail and Nuclear Balance. Washington, D.C.: The Brookings Institution, 1987.
- Cebrowski, Vice Admiral Arthur Garstka, John J., "Network-Centric Warfare-Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 28-35.
- Chairman of the Joint Chiefs of Staff, Joint Vision 2010 Washington: 1996
- Chairman of the Joint Chiefs of Staff, National Military Strategy Washington: 1997
- Defense Science Board 1997 Summer Study Task Force. DoD Responses to Transnational Threats. Washington, D.C.: October 1997.
- Ekeus, Rolf, "Beware Iraq's Biowar Legacy." Jane's IDR Extra, Vol. 2, No. 2, February 1997, Viewpoint.
- Frank Gaffney Jr, "Biological Warfare Warning," Washington Times, April 28, 1998, pg 21.
- Johnson, Stuart E., ed. The Niche Threat, Deterring the Use of Chemical and Biological Weapons. Washington, DC: National Defense University Press, 1997
- Kissinger, Henry A. Nuclear Weapons and Foreign Policy. New York: Harper & Brothers, 1957.
- Krepinevich, Andrew F, "Calvary to Computer: The Pattern of Military Revolutions" in Strategy and Force Planning, edited by Strategy and Force Planning Faculty. Newport War College Press, Newport RI, 1997.

Molander, Roger C., Riddile, Andrew S., Wilson, Peter A. Strategic Information Warfare. Santa Monica, CA: RAND, 1996.

Norris, Robert, S., "To Nuke or Not to Nuke." The Bulletin of the Atomic Scientists, January/February 1994, 64.

"Observations on the Emergence of Network-Centric Warfare." Information Paper. <<http://www.dtic.mil/jcs/j6/education/warfare.html>> (27 Apr 98).

Office of the Secretary of Defense, Proliferation: Threat and Response, April 1996
Washington: 1996.

Office of the Secretary of Defense, Report of the Quadrennial Defense Review, May 1997
Washington: 1997.

Reid, Brian Holden. "J.F.C. Fuller's Theory of Mechanized Warfare," The Journal of Strategic Studies, December 1978, Vol. 1, No. 3, pp. 295-312.

"Report: U.S. Germ Attack Simulation a Disaster," New York Times, April 26, 1998.

U.S. Joint Chiefs of Staff. Doctrine for Joint Nuclear Operations (Joint Pub 3-12) Washington, D.C.: December 18, 1995.

U.S. Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (Joint Pub 6-0) Washington, D.C.: 30 May 1995, pg. II-1.

United States Naval War College, On Operational Art. Newport: 1998.

Warden, Colonel John A., USAF, "The Enemy as A System," Airpower Journal, Spring 1995, pg 41-55.

White House. A National Security Strategy For A New Century. Washington, D.C.: May 1997.